

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

## In the Matter of the Search of

*(Briefly describe the property to be searched  
or identify the person by name and address)*THE RESIDENTIAL BUILDING, ANY OUTBUILDINGS, ANY  
APPURTENANCES THERETO, ANY VEHICLES, ANY PERSONS,  
ASSOCIATED WITH THE PROPERTY LOCATED AT 1210 VALLEY VIEW  
ROAD, GREEN BAY, WI 54304; AND FOR REDDIT ACCOUNT "96jax."

Case No. 24-m-017

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

See Attached Affidavit (Paragraph 3)

The application is based on these facts:

See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of        days *(give exact ending date if more than 30 days: \_\_\_\_\_)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Davis Mendelsohn

Applicant's signature

DAVIS MENDELSON, SA HSI

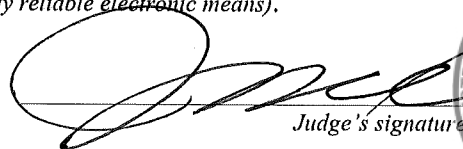
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
*(specify reliable electronic means).*

Date:

2-8-24

City and state: Green Bay, Wisconsin



Judge's signature

Hon. James R. Sickel, Magistrate Judge



**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION FOR A SEARCH WARRANT**

I, Davis Mendelsohn, being duly sworn, state as follows:

**INTRODUCTION**

1. I make this affidavit in support of an application for two search warrants:
  - a. A search warrant under Federal Rule of Criminal Procedure 41(b)(1) to search the locations described further in Attachment A-I, which include the property of 1210 Valley View Road in Green Bay, Wisconsin, a property within Brown County in the Eastern District of Wisconsin (the “SUBJECT ADDRESS”), as well as the person of Bryan PETERSON and PETERSON’s dark gray Ford Escape with Wisconsin license plate AFL3995, to the extent that such person or vehicle are located within the Eastern District of Wisconsin at the time the warrant is executed (collectively, the “SUBJECT LOCATIONS”), for the items listed in Attachment B-I.
  - b. A search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A), and 2703(d) to require Reddit Inc. (hereinafter the “PROVIDER”), a provider of electronic communication and remote computing services headquartered in San Francisco, California, to disclose to the government copies of the information (including the content of communications) associated with the Reddit account “96jax” (the “SUBJECT ACCOUNT”). The SUBJECT ACCOUNT is further described in Attachment A-II and the information to be provided by the PROVIDER is further described in Section I of Attachment B-II.<sup>1</sup> Upon receipt of the information described in

---

<sup>1</sup> Because this Court has jurisdiction over the offense(s) being investigated, it may issue the warrant to compel the PROVIDER pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). See 18 U.S.C. §§ 2703(a) (“A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by

Section I of Attachment B-II, law enforcement agents and/or individuals assisting law enforcement and acting at their direction will review that information to locate the items described in Section II of Attachment B-II.

2. Attachments A-I, B-I, A-II, and B-II are incorporated herein by reference.

3. As described more fully below, I respectfully submit there is probable cause to believe the items and information associated with the SUBJECT LOCATIONS and SUBJECT ACCOUNT constitutes contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 371 (conspiracy); 2251(a), (d), and (e) (sexual exploitation of a minor by production and advertisement of child pornography, and conspiracy and attempt to commit such offenses); 2252(a)(1), (a)(2), (a)(4)(B), (b)(1), and (b)(2) (transportation, distribution, receipt, access with intent to view, and possession of child sexual abuse material ("CSAM"), and conspiracy and attempt to commit such offenses); 2252A(a)(1), (a)(2), (a)(3), (a)(5)(B), (b)(1), and (b)(2) (transportation, distribution, receipt, pandering, access with intent to view, and possession of CSAM, and conspiracy and attempt to commit such offenses); and 2422(b) (enticement of a minor to engage in criminal sexual conduct) (collectively, the "TARGET OFFENSES"). The locations to be searched are described in more detail in the following paragraphs and in Attachment A, and the items to be seized are more specifically described in Attachment B.

4. This affidavit is intended to merely show that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The statements in this affidavit are based on information provided to me by other law enforcement

---

a court of competent jurisdiction") and 2711 ("the term 'court of competent jurisdiction' includes -- (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that -- (i) has jurisdiction over the offense being investigated...").

officials, witnesses, and documents and evidence I have reviewed, as well as my investigation of this matter.

5. Based on my training and experience and the facts set forth in this affidavit, I believe there is probable cause that PETERSON has committed violations of the TARGET OFFENSES. There is also probable cause to search the SUBJECT LOCATIONS and the SUBJECT ACCOUNT, further described in Attachments A-I and B-I, for evidence, instrumentalities, and fruits of the TARGET OFFENSES, further described in Attachments A-II and B-II.

#### **AFFIANT BACKGROUND**

6. I have been a special agent (SA) with Homeland Security Investigations (HSI), the investigative component of the United States Department of Homeland Security's Immigration and Customs Enforcement (ICE), since January 2019. I am currently assigned to HSI's Office of the Resident Agent in Charge in Monterey, California. As part of my daily duties, I investigate violations of federal laws concerning the sexual exploitation of children. Prior to my employment with HSI, beginning in June 2016, I was a sworn investigator with the California Department of Motor Vehicles (DMV). While employed with the DMV, I conducted investigations related to a variety of criminal and administrative offenses.

7. Throughout my law enforcement career, I have received training on conducting criminal investigations, search and seizure laws, and the authoring of probable cause affidavits. In 2017, I completed a 24-week-long basic police academy in California, and in 2019, I completed the Criminal Investigator Training Program and HSI Special Agent Training program, a total of 26 weeks of training, at the Federal Law Enforcement Training Center in Brunswick, Georgia. Since becoming a federal law enforcement officer, I have written probable cause

affidavits in support of multiple federal search warrants and complaints for cases involving the sexual exploitation of children.

### **DEFINITIONS**

8. The following definitions apply to this affidavit and Attachment B:

a. **Chat:** Any kind of text communication over the Internet that is transmitted in real time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. **Child Erotica:** Any materials or items that contain sexualized depictions or descriptions of minors, or that are sexually arousing to persons having a sexual interest in minors, but which are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

c. **Child Pornography:** As defined in 18 U.S.C. § 2256(8)(a) and referred to as “child sexual abuse material,” or “CSAM,” throughout this affidavit, any visual depiction of sexually explicit conduct where ... the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct...

d. **Computer:** Defined by 18 USC § 1030(e)(1) and refers to “an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions.” The term “computer” includes any data-storage facility and communications facility directly related to or operating in conjunction with such device as well as smartphones and mobile phones.

e.       **Computer Hardware:** Equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input and output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); and any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f.       **Computer Passwords and Data Security Devices:** Information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) is usually digital key used to access particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain preset security functions when touched. Data security software or code may also encrypt, compress, hide, or “boobytrap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g.       **Computer Software:** Digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. **Computer-Related Documentation:** Written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. **Internet:** A global network of computers and other electronic devices that communicate with each other. Connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

j. **Internet Connection:** A connection required for access to the Internet. The connection is generally provided by cables, digital subscriber lines, wireless devices, or satellite systems.

k. **Internet Protocol (IP) Address:** A unique number used by a computer or other digital device to access the Internet. IP addresses can be “dynamic,” meaning that the internet service provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

l. **Minor:** Defined in 18 USC § 2256(1) and refers to any person under 18 years of age.

m. **Sexually Explicit Conduct:** Defined in 18 USC § 2256(2)(A) and means actual or simulated sexual intercourse (including genital-genital, oral-genital, anal-genital, or oral-anal), whether between persons of the same or opposite sex, bestiality, masturbation, sadistic or masochistic abuse, or lascivious exhibition of the anus, genitals, or pubic areas of any person.

n. **Storage Medium:** Any physical object, such as hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media, upon which computer data can be recorded.

o. **Visual Depictions:** Defined in 18 USC § 2256(5) and includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

p. **Wireless Network:** A system of wireless communications in which signals are sent and received via electromagnetic waves such as radio waves. Each person wanting to connect to a wireless network needs a computer which has a wireless network card that operates on the same frequency as the wireless network. Many wired networks base the security of the network on physical access control, trusting all users on the local network. However, if wireless access points are connected to the network, anyone in proximity to the network can connect to it. A wireless access point is equipment that connects to the modem and broadcasts a signal. It is possible for an unknown user who has a computer with a wireless access card to access an unencrypted wireless network. Once connected to that network, the user can access any resources available on that network to include other computers or shared Internet connections.

## **BACKGROUND TO THE INVESTIGATION**

### **SUMMARY**

9. In January 2024, while acting in an undercover capacity, I began investigating an online chat group ("Chat Group 1") on an encrypted chat application ("Chat Application A")



after the creator of Chat Group 1 added me to the group.<sup>2</sup> As of February 1, 2024, Chat Group 1 is active with over 40 members. Based on Chat Group 1's name and content, I determined Chat Group 1's theme is "grooming," a term that refers generally to the process of developing a relationship with a minor for the purpose of increasing the minor's receptiveness to sexual activity with an adult. Specifically, in Chat Group 1, users discuss attempts to use the internet to communicate with minors for sexual purposes, exchange usernames of potential minor victims, and share sexually explicit images and videos depicting alleged minor victims.

10. Some members of Chat Group 1, including a user I identified using the label "S-3," stated that they use Snapchat to attempt to entice minor victims to send them sexually explicit content of themselves. In Chat Group 1, S-3 stated he uses the internet to groom minors for sexual purposes and sent sexually explicit images of females he claimed were minors. For the reasons set forth in this affidavit, there is probable cause to believe S-3 is Bryan PETERSON, a 45-year-old male residing at the SUBJECT ADDRESS in Green Bay, Wisconsin.

#### OVERVIEW OF CHAT APPLICATION A

11. Based on my training, experience, and knowledge of this investigation, I know the following about Chat Application A:

- a. Chat Application A is an encrypted chat application that is available for both mobile and desktop devices and can run on iOS, Android, and Windows operating systems. Users do not need to provide a phone number or email address to create an account on Chat Application A. Chat Application A's website boasts that Chat

---

<sup>2</sup> I know the names of Chat Application A and Chat Group 1 and the Chat Application A usernames and identification numbers of all users discussed in this affidavit. However, because the investigation into Chat Application A and Chat Group 1 remain active, these and other sensitive operational details have been omitted from this affidavit to protect operational security and decrease the likelihood that the investigation into Chat Group 1 becomes prematurely known by its users.

Application A protects data through end-to-end encryption, does not retain any metadata or IP addresses, and only stores messages until their delivery. Because of this encryption, certain information that is often obtainable from companies such as the PROVIDER – such as customer names, email addresses, phone numbers, and logs of IP addresses used to access the application – is not obtainable from the company behind Chat Application A.

b. The above-described encryption means users of applications like Chat Application A are difficult to identify. The privacy and protection provided by encrypted chat applications makes them popular among those engaged in crimes such as activity related to the sexual abuse of children and producing, distributing, and possessing CSAM. Users of these applications tend to know they can operate with a higher level of anonymity than they can on unencrypted messaging applications. Chat Application A users can choose display names, have unique identification numbers, and can communicate with one another in groups or privately, one on one.

#### S-3's PARTICIPATION IN CHAT GROUP 1

12. On January 3, 2024,<sup>3</sup> the creator of Chat Group 1 (“S-1”) added me to the group.<sup>4</sup> That same evening, a member of the group replied to an earlier message sent by S-3 by stating, “That pussy looks amazing.” In this user’s reply, I could see a portion of S-3’s original message, which included image thumbnails and the text, “[Part of female’s first name] 13.” However,

---

<sup>3</sup> Unless otherwise noted, all dates and times in this report are according to California time.

<sup>4</sup> This section of the affidavit includes only selected information from Chat Group 1 in order to establish probable cause for the requested warrants. It does not include all information, chats, and photos from Chat Group 1.

because the original message and images were sent by S-3 prior to me joining the group, I could not see the full images or message.

13. On January 4, 2024, I asked in Chat Group 1 for someone to resend the images previously sent by S-3. S-1 then resent the images, which included what appears to be an image of a postpubescent female naked from the waist down, spreading her legs to expose her vagina to the camera. The full text from the original message stated “[part of female’s first name] 13 Denmark.” Based on the context of the message and the content I have since reviewed in Chat Group 1, I understand “13” to be a reference to the age of the female depicted in the images.

14. That same day, when another group member (“S-2”) asked in Chat Group 1 whether anyone uses a specific social media application for “grooming,” S-3 replied, “I do.” After another user asked if anyone had experience with grooming “black girls,” S-3 stated he did, specifying, “I have in person not online.” S-2 then sent, “Anyone want the snap of a 13yr old i know. Maybe see if you can get some nudes etc?” S-3 answered S-2’s question by stating, “Dm [short for “direct message”] me I’ll try.”

15. On January 5, 2024, S-3 posted multiple images of a postpubescent female with the message, “16 from Canada.” One of the images shows the female on the floor, her buttocks facing the camera, grabbing one side of her buttocks to expose her vagina and anus to the camera. Another image depicts what appears to be the same female naked from the waist down. She is depicted from the back while bending forward, again spreading her buttocks to expose her naked vagina and anus. Other users of Chat Group 1 responded to S-3’s post to say, “love the stretched ass,” “That’s hot asf” (abbreviation for “as fuck”), and, “Canadian girls are sluts that’s what I can tell you.”

16. On January 8, 2024, S-3 posted multiple images of a postpubescent female with the message, "13to [female's first name]." From my training, experience, and understanding of Chat Room 1, I know the letters "yo" after a number generally mean "years old" and refer to the age of a person. Based on the context, I believe "13to" is a typo for "13yo." Four of the images showed the female exposing her breasts to the camera, and two images showed the female standing in front of a mirror, nude, with both of her breasts exposed, and her pubic area partially exposed. After S-1 asked S-3 where he found the female, S-3 named a specific application, then stated, "I don't do anything on [application name] accept [except] chat. Then I switch to snap for the grooming." When another user asked, "Do you come across many younger kids on there ?" S-3 replied, "My wheel house is teens. But yes I've seen way younger." S-3 added the following message regarding his experience with the social media application he previously mentioned:

Snaps algorithms look for now [believed to be "known"] content. Like if you were posting [female's first and last name] or one of those type of models. They do t [believed to be "don't"] really look at other snaps unless a complaint is made. Sign up with a temporary email and always use a vpn.

Based on my training and experience, I know a "virtual private network," or "VPN," is a way for users to access the internet in a way that prevents website servers from seeing their true IP address. S-3 also stated, with respect to a different application, "[y]ou gotta swipe through a lot of Dicks but you'll find lots of girls if you're patient."

17. On January 9, 2024, another member of Chat Group 1 posted a recording, over 15 minutes in length, of a video chat showing a female who appears to be approximately 10-to-13 years old reacting to various videos of the sexual abuse of children, including prepubescent children. For example, during a portion of the recording, the 10-to-13-year-old female appears to react to a video showing a female, approximately nine-to-11 years old, pulling the pants off a postpubescent male before orally copulating his penis. Approximately five minutes later, after

other users discussed the 10-to-13-year-old female from the recording, S-3 stated, “For real I wish o [believed to mean “I”] would’ve found her.”

18. On January 10, 2024, another member of Chat Group 1 posted over 30 images of young minors, some of which are described below:

- a. An image depicting a postpubescent male having anal intercourse with a prepubescent female.
- b. An image depicting a prepubescent female, approximately two-to-three years old, lying on her back, nude, with what appears to be male ejaculate covering her stomach and vagina. The image was taken by a postpubescent male, and his erect penis is near the female’s vagina in the image.
- c. An image depicting a female, approximately three-to-four years old, orally copulating the penis of a postpubescent male.
- d. An image depicting a prepubescent female, approximately two-to-four years old, lying on her back, nude with her legs spread apart, vagina displayed to the camera, and each of her hands forced away from her body from being tied to something out of frame.

In response to these posts, S-1 stated, “Just a reminder, this is a group for sharing original content only.” I am aware that, in the CSAM context, “original content” refers to CSAM that a user himself produced or was involved in producing.

19. On January 11, 2024, S-1 posted multiple images of a female followed by the message, “[Female’s name], 12, Czech Republic.” Some of the images showed the female’s face, and two showed her bare breasts. In response, S-3 commented, “Perfect teen tits.”

20. On January 12, 2024, S-3 posted three images of a female, approximately 12-to-16 years old, posing in front of a mirror wearing nothing aside from underwear. SA Mendelsohn asked S-3 where he found her, but received no response.

21. On January 31, 2024, S-3 posted multiple images of a female followed by the message, "My newest target 14 from Texas." One of the images depicts the female with her shirt hiked up, displaying her bare breasts, and another image depicts a close-up view of a female's vagina with no visible pubic hair growth. Based on my training and experience and the context of Chat Group 1, I believe S-3 was referring to the female's age when he wrote, "14."

22. Throughout the general timeframe set forth above, users of Chat Group 1 other than S-3 made comments that referred to underage girls. These comments included the following: "Anyone want the snap of a 13yr old i know. Maybe see if you can get some nudes etc?"; "Had lots of luck with girls from about 10 to 14! ... Been lucky enough to cam with a lot of 13 and 12 yo... Some show themselves and play but most just like to watch u wank"; "I'm talking to a 13 yo I met on [platform]"; "There's lots of underage girls on there..."; "big tits for 12"; "All little girls are secretly sluts"; "I have a girl I'm talking to" who is "14 allegedly." The users of Chat Group 1 also shared images of females, some of which included nudity. As noted above, some of the depicted females were sexually mature, but nearly all of them included numbers that appeared to be ages, including three, 11, 12, 13, and 16.

#### S-3's PARTICIPATION IN ANOTHER GROUP IN CHAT APPLICATION A

23. S-3 is a member of at least one other group on Chat Application A that I have been monitoring. While I do not know when S-3 joined the group, he has participated in this group by posting messages on as early as January 22, 2024. Since then, users have posted videos and images depicting the sexual abuse of children. For example:

a. On January 22, 2024, a user posted a video, approximately 14 seconds long, of a postpubescent male having sexual intercourse with a child who appears to be under 10 years old. In the video, the small-framed child, who is crying, is face down on his or her stomach while the male is on top of him or her, holding his or her arms.

b. On January 24, 2024, a user posted multiple images of a minor female, approximately six-to-nine years old. In some of the images, the female was spreading her legs, displaying her bare vagina to the camera.

c. On January 26, 2024, a user posted an image depicting a male ejaculating on the face of a child who appears to be approximately seven-to-10 years old.

PRIVATE MESSAGES WITH S-3 ON CHAT APPLICATION A

24. On January 9, 2024, after S-3 accepted my request to privately message him on Chat Application A, I sent S-3, "Hey man. If you wanna trade one Snap username for another, lemme know." S-3 responded, "I've got one I haven't been about [believed to be "able"] to crack yet if you want to give her a try." After I asked if he wanted to trade that username for one I had, S-3 said, "Yes let's trade," then sent me a Snapchat username. I subsequently sent S-3 the Snapchat username for a Snapchat account under my control ("UC Account 1"), which appeared to be the Snapchat account of a female.

25. Within 10 minutes, I received a friend request on UC Account 1 from a specific Snapchat account ("Snapchat Account 1"). Then, on Chat Application A, S-3 said, "Mine is [Snapchat Account 1 username] if you want to tell her."

26. That same day, I asked S-3, "You have any actual experience with girls in real life?" S-3 responded, "Yes. I have one that I've been fucking irl [short for "in real life"] for six months. And one that I hooked up with twice." I asked S-3 how old they were, but received no

response from S-3 for the remainder of the day. The next day, S-3 replied, "14," then sent another message stating, "And 13." I asked S-3 where he met them and how old he was, and S-3 claimed he met them on Reddit and that he was 45 years old.

27. On January 10, 2024, I posted an age-regressed, selfie-style image of an undercover HSI agent in Chat Group 1. Because of the age-regression, this image appeared to depict a minor girl with blonde hair. I then told users to message me if they wanted this "girl's" Reddit username. Shortly thereafter, I sent S-3 a private message that included a screenshot of a Reddit profile controlled by me ("UC Account 2") and stated, "Well here's the chick I've been talking to on Reddit if you wanna take a stab at her too lol." S-3 said he would try, then stated, "They are fun to play with. And they are pleasers." S-3 subsequently asked if I had gotten any pictures of "her" (referring to the "chick" from Reddit), then said, "I see is that the little blonde you posted [in the] other chat," referring to the age-regressed image of the undercover HSI agent I previously posted in Chat Group 1. I confirmed, "Yeah it's the blonde," but received no response from S-3.

28. I later asked S-3, "You hit her up yet?" S-3 stated he had not received replies from either UC Account 1<sup>5</sup> or UC Account 2. When I replied, "Hmm I'm talking to the one from Reddit now and no one else has messaged her," S-3 stated he would try again, then stated, "It says failed to send chat." I then said, "I can give her your username if you want." S-3 subsequently sent me the username for the SUBJECT ACCOUNT. When I tried to visit the public profile for the SUBJECT ACCOUNT, the webpage stated, "This account has been

---

<sup>5</sup> While acting in an undercover capacity, I have since used UC Account 1 to communicate with S-3 on Snapchat. In these conversations, S-3 claimed to be 18 years old and from Chicago. S-3 also asked, "You got a bf [short for 'boyfriend']?" However, as of February 1, 2024, I have not yet told S-3 an age for my undercover persona on UC Account 1.



suspended.” Based on my training and experience, social media websites like Reddit sometimes ban or suspend accounts that violate the website’s terms of service. I also know Reddit’s terms of service include a rule prohibiting “any sexual or suggestive content, and predatory or inappropriate behavior, involving minors (i.e., people under 18 years old) or someone who appears to be a minor.” Therefore, I believe it is possible, although not certain, that Reddit suspended the SUBJECT ACCOUNT based on the user’s violation(s) of Reddit’s policies regarding predatory or inappropriate behavior involving minors.

29. On January 25, 2024, on Chat Application A, I asked S-3 how it was going with the female he stated he had “been fucking irl for six months.” S-3 stated it was going “pretty good.” S-3 confirmed he met the female through Reddit. When I asked, “How did you get her from there to in person,” S-3 responded, “Switched to [social media application] and groomed her there.” S-3 also told me he found the female on an “age gap” portion of Reddit and that she lived a couple of hours away from him.

#### IDENTIFICATION OF S-3 AS BRYAN PETERSON

30. On January 16, 2024, in response to a United States Department of Homeland Security (DHS) summons, the PROVIDER produced subscriber and address information associated with the SUBJECT ACCOUNT. The data from the PROVIDER reported the SUBJECT ACCOUNT had a creation date of April 28, 2023 (UTC). The data further reported a specific IP address (“IP Address 1”) was associated with account activity approximately 168 times between October 2023 and January 2024 and another specific IP address (“IP Address 2”) was used to register the account and was associated with account activity approximately eight additional times between October 2023 and December 2023. Through open-source internet

searches, I determined IP Address 1 belonged to AT&T and IP Address 2 belonged to Charter Communications.

31. On January 23, 2024, in response to a DHS summons, AT&T produced subscriber information for IP Address 1 and multiple other IP addresses on specific dates and times the IP addresses were associated with the SUBJECT ACCOUNT. The data from AT&T reported the subscriber associated with each listed IP address as Bryan PETERSON at the SUBJECT ADDRESS.<sup>6</sup> Further, AT&T provided a specific phone number (“Phone Number 1”) as associated with PETERSON’s account.

32. I then searched PETERSON’s name and date of birth in a government database and located PETERSON’s Wisconsin driver’s license information, which listed PETERSON’s date of birth as May 11, 1978, and included a “primary contact address” of the SUBJECT ADDRESS. Using open-source internet searches, I located PETERSON’s Facebook page, which listed “Worked at [name of high school],” “Worked at Oneida West Mason Street Casino,” “Former Security Officer at Oneida Casino,” and that he currently lives in Green Bay, Wisconsin. Where “Former Security Officer at Oneida Casino” was listed, Oneida Casino was also tagged, allowing users to click on the name to visit Oneida Casino’s Facebook page, which listed its address as 2020/2100 Airport Drive in Green Bay.

33. Through open-source searches, I also located PETERSON’s LinkedIn page, which reported his experience as “Head Football Coach – Varsity” at the same high school listed in his Facebook page from September 2008 to present and “Judicial Security Office” at Oneida Tribe of Indians of Wisconsin Government from December 2000 to present. I subsequently

---

<sup>6</sup> The data from AT&T listed the SUBJECT ADDRESS as being in Ashwaubenon, Wisconsin. According to open-source information, Ashwaubenon is a suburb of Green Bay, Wisconsin.

located another LinkedIn page for PETERSON, which reported his experience “Bailiff” at “Oneida Tribe Of Indians Of Wisconsin Governmen[t]” without a date range, “Head Coach/General Manager” for a semi-professional football team from 2018 to present, and “Head Football Coach” at a specific school from 2008 to October 2020.

34. On January 24, 2024, in response to a DHS summons, Charter Communications produced subscriber information for IP Address 2 on specific dates and times it was associated with the SUBJECT ACCOUNT. The data from Charter Communications reported the subscriber of the IP address was Oneida Nation Casino at 2020 Airport Drive, Stop 3, in Green Bay. The 2020 Airport Drive address matched the address for Oneida Casino’s Facebook page linked by PETERSON’s Facebook page.

35. On January 24, 2024, in response to a DHS summons, Snap Inc. produced data associated with Snapchat Account 1, the account S-3 provided to me. The account data listed Phone Number 1 as associated with Snapchat Account 1. According to the IP address data provided by Snap Inc., IP Address 1 was associated with Snapchat Account 1 activity approximately 583 times between November 2023 and January 2024, and IP Address 2 was associated with Snapchat Account 1 activity approximately 99 times between November 2023 and December 2023. As described earlier, both of those IP addresses were also associated with the SUBJECT ACCOUNT, and IP Address 1 was assigned to the SUBJECT ADDRESS.

36. On January 26, 2024, in response to a DHS summons, UScellular produced subscriber information for Phone Number 1, the number associated with PETERSON’s AT&T account and Snapchat Account 1. The data produced by UScellular reported Bryan PETERSON with a date of birth of May 11, 1978, as the subscriber associated with the phone number. The

data listed the SUBJECT ADDRESS<sup>7</sup> as a billing and primary address associated with Phone Number 1.

SEARCH WARRANT FOR DATA ASSOCIATED WITH SNAPCHAT ACCOUNT 1

37. On January 26, 2024, in response to a federal search warrant signed by United States Magistrate Judge Jean Rosenbluth of the United States District Court for the Central District of California (case number 2:24-MJ-00284),<sup>8</sup> Snap Inc. provided data, including message content and location data, associated with Snapchat Account 1. Many of the messages to and from S-3 were sexual in nature. In my preliminary review of the data, I observed the following:

- a. On December 6, 2023, S-3 told another user he lived in Green Bay.
- b. On December 8, 2023, S-3 introduced himself to another user as “Bryan.”
- c. On December 15, 2023, S-3 told another user, “I’m gonna leave bit makes [marks] and hickeys on those little tits.”
- d. On December 16, 2023, another user sent S-3, “oh hey bryan!”
- e. On January 10, 2024, S-3 asked another user, “Is school capable of teaching you to be the best slut you can?”
- f. Multiple images from a user showing a female’s face and breasts.

Additionally, at least one image from the same user showed a female spreading her legs

---

<sup>7</sup> The data also listed two other addresses (one billing and one primary) as associated with Phone Number 1. The data did not include dates with any of the addresses.

<sup>8</sup> At the time Judge Rosenbluth signed the search warrant, I had not yet identified PETERSON as S-3 or confirmed where S-3 was located. Therefore, I obtained the search warrant from the Court in the same district as Snap Inc.’s headquarters.

to display her postpubescent vagina to the camera. Based on my review of the images, I believe the female is a minor teenager or a younger adult.

g. GPS coordinates showing the location of Snapchat Account 1's user as the SUBJECT ADDRESS on January 10, 2024 (UTC).

#### SURVEILLANCE IN WISCONSIN

38. On the morning of January 30, 2024, an HSI agent in Wisconsin conducted surveillance at the SUBJECT ADDRESS and observed a dark gray Ford Escape and a light-colored Chevy Malibu in its driveway. The agent was unable to obtain the license plate of the Ford Escape, but did obtain the license plate of the Chevy Malibu. Government records showed the Malibu as registered to a female subject at the SUBJECT ADDRESS. Additionally, records from a commercial database reported a gray Ford utility vehicle with Wisconsin license plate AFL3995 as associated with PETERSON. Shortly after the agent originally saw the Ford Escape at the SUBJECT ADDRESS, he noticed it was no longer there.

39. Later that morning, the agent located a dark gray Ford Escape (Wisconsin license plate AFL3995) in the parking lot of the Oneida Judiciary Courts. Government records showed the Escape as registered to PETERSON at the SUBJECT ADDRESS.

#### SUMMARY OF INVESTIGATIVE FINDINGS

40. As described in this affidavit, S-3 is a member of Chat Group 1 – a group dedicated to discussions and content regarding the grooming of minors for sexual purposes – and, in the group, stated he uses the internet for such purposes. Furthermore, in Chat Group 1, S-3 shared sexually explicit images of two females he claimed were 13 years old, one female he claimed was 16 years old, and one female he claimed was 14 years old. In private messages with me while I was acting in an undercover capacity, S-3 claimed he was sexually active with a

minor he met using Reddit and specified in which section of Reddit he found the minor.

Additionally, S-3 is a member of another group on Chat Application A in which users regularly share images and videos showing the sexual abuse of children.

41. Further, S-3 used Snapchat Account 1 to send a friend request to UC Account 1, and he sent me the username to his Reddit account, the SUBJECT ACCOUNT. When I attempted to view the SUBJECT ACCOUNT's public profile, I learned it was suspended. Based on my training, my experience, and what S-3 told me about his use of Reddit, I believe it is possible the PROVIDER suspended the SUBJECT ACCOUNT because of S-3's violation of the PROVIDER's rules regarding inappropriate behavior regarding minors. The data I obtained from Snap Inc. and the PROVIDER, such as IP address data, indicate both Snapchat Account 1 and the SUBJECT ACCOUNT point back to Bryan PETERSON. Because PETERSON appears to have accessed the SUBJECT ACCOUNT from various IP addresses – including multiple that resolve to his home, the SUBJECT ADDRESS, and one that resolves to his possible workplace – it is likely he has at least one mobile or easily moveable device that he has used to commit the SUBJECT OFFENSES. Based on my training and experience, I know people often keep electronic devices, such as cell phones, laptops, tablets, and electronic storage devices, on their person (e.g., in their pockets or in storage bags), in their vehicles, and/or in their residences.

42. Additionally, when an HSI agent in Wisconsin conducted surveillance at the SUBJECT ADDRESS, he saw a gray Ford Escape – matching the description of PETERSON's Ford Escape – parked in the driveway. The agent later observed a gray Ford Escape – matching the description of the one previously at the SUBJECT ADDRESS and registered to PETERSON – parked in the parking lot of PETERSON's possible workplace.

43. Based on my training and experience, subjects who engage in online enticement with minors, as S-3 has claimed to do, often use multiple accounts from the same social media applications to do so. I have personally investigated subjects who used multiple Reddit accounts to communicate with minors. Additionally, from my training and experience, I know those who sexually exploit children often do so over long periods of time and with multiple victims, either simultaneously or one after another. Therefore, based on the information specific to S-3 contained within this affidavit and my general knowledge related to those who use the internet and social media to sexually exploit children, I believe reviewing the contents of the SUBJECT ACCOUNT as well as items and electronic evidence located in/at the SUBJECT LOCATIONS may lead to the discovery of multiple potential minor victims and further evidence of the SUBJECT OFFENSES.

**BACKGROUND REGARDING COMPUTERS,  
CHILD EXPLOITATION, AND THE INTERNET**

44. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, knowledge, and conversations with other law enforcement personnel familiar with these types of investigations, I know the following:

1. Computers and digital technology have dramatically changed the way in which individuals interested in sexually exploiting children interact with each other. Computers serve multiple functions in connection with child exploitation, including allowing people engaging in child exploitation to communicate and allowing for the production, distribution, and storage of child pornography. People engaged in seeking out children to exploit on the Internet will often store images of the exploited child in electronic format.

2. A computer's ability to store images in digital form makes the computer itself an ideal repository for images of child exploitation. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. Large-capacity external and internal hard drives are common. Other media-storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, all which are very small devices that are plugged into a port on the computer. Additionally, it is extremely easy for an individual to take a photo or a video with a digital camera or smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to media-storage devices. Media-storage devices can easily be concealed and carried on an individual's person or in their vehicle. Mobile phones, including smart phones, can act as media-storage devices and are also often carried on an individual's person or in an individual's vehicle.

3. The Internet offers those involved in the sexual exploitation of children several different venues to meet and communicate as well to obtain, view, and trade child pornography, all in a relatively secure and anonymous fashion.

4. Individuals can use online resources (such as Yahoo! and Gmail, among others) to communicate regarding child exploitation and retrieve and store child pornography. These online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used,



however, evidence of the exploitation of minors using the Internet, such as child pornography, can be found on the user's computer or external media in most cases.

5. As is the case with most digital technology, communication by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (i.e., saving an email as a file on the computer or saving the location of one's favorite websites in "bookmarked" files). Digital information can also be retained unintentionally. For example, traces of the path of an electronic communication may be automatically stored in many places. In addition to electronic communications, a computer user's Internet activities generally leave traces in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

#### **SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

45. Based on my training, experience, and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macro-SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including, but not limited to, "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for several reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer

hardware and software in use today that it is impossible to bring to the search site all the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures that are designed to maintain the integrity of the evidence and to recover hidden, erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “boobytraps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises.

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a dongle or keycard, is necessary to decrypt the data into a readable form. In addition,

computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography, a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

46. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for contraband or evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system’s input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve the system’s data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

- a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input and output devices in order to read the data on the system. It is important that the analyst be able to properly reconfigure the system to accurately retrieve the previously mentioned evidence. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers), any applications software which may have been used to create the data (whether stored on hard drives or on external media), and all related instruction manuals or other documentation and data security devices.

b. To fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). In cases where the evidence consists partly of image files, the monitor and printer are also essential to show the nature and quality of the graphic images the system could produce. Further, as previously stated, the analyst needs all the system software (operating systems or interfaces and hardware drivers) and any applications software which may have been used to create the data, whether stored on hard drives or on external media, for proper data retrieval.

47. Additionally, based on my training, experience, and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to wirelessly connect to the Internet. Wireless networks may be secured (a user must enter an alphanumeric key or password before gaining access to the network) or unsecured (a user may access the wireless network without a key or password). Wireless routers for both secured and unsecured wireless networks may yield significant evidence or serve as instrumentalities of a crime. For example, a wireless router may serve as the instrument through which the perpetrator of an Internet-based crime connected to the Internet and might contain information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

48. Based on my training and experience, I know that graphic image files sent and received during the online exploitation of children, including those containing child pornography, can be maintained for long periods of time on the aforementioned media-storage devices. An individual who has a sexual interest in children often maintains these files purposefully and uses the images for sexual gratification. Even when the image files have been deleted, computer forensic experts are often able to recover the images that had been previously possessed.

49. Based on my training and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools.

50. Based on my training and experience, I know that data (particularly images) can be received by use of a home computer and transferred to other electronic devices, such as a cell phone. I also know that data or images can be received by a cell phone and transferred to a home computer or other electronic-storage devices.

### **BIOMETRIC UNLOCK FEATURES**

51. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the

user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress PETERSON's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of PETERSON's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

#### **BACKGROUND ON SOCIAL MEDIA ACCOUNTS**

52. In my training and experience, I have learned that providers of social media services offer a variety of online services to the public. Companies like Reddit allow subscribers to obtain accounts like the SUBJECT ACCOUNT. Subscribers obtain an account by registering with providers. During the registration process, providers generally ask their subscribers to provide certain personal identifying information when registering for an account. Such information can include the subscriber's full name, physical address, phone numbers and other

identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of an account.

53. Therefore, the computers of Reddit are likely to contain stored electronic communications and information concerning subscribers and their use of the services of Reddit, such as account access information, email or message transaction information, and account application information. From my training and experience, I know such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of the SUBJECT ACCOUNT.

54. From my training and experience, I know social media providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service(s) utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, social media providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the SUBJECT ACCOUNT.

55. From my training and experience, I know social media account users will sometimes communicate directly with service providers about issues relating to the account, such

as technical problems, billing inquiries, or complaints from other users. Providers of social media services typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. Such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of the SUBJECT ACCOUNT.

56. Providers of social media often maintain, have access to, and store information related to the location of the users of accounts they service. That information may be obtained by the provider in a number of ways. For example, a user may access the provider's services by running an application on the user's phone or mobile device. This application may have access to the location information residing on the phone or mobile device, such as Global Positioning System (GPS) information. It may also be accessible through "check-in" features that some providers offer that allow users to transmit or display their location to their "friends" or "acquaintances" via the provider. In this particular investigation, location data associated with the SUBJECT ACCOUNT can assist investigators with confirming whether or not PETERSON is truly the user of the SUBJECT ACCOUNT. For example, location data associated with the SUBJECT ACCOUNT can be cross referenced with information such as known addresses associated with PETERSON. Furthermore, location data can assist investigators with determining PETERSON's whereabouts when he committed the SUBJECT OFFENSES.

#### **BACKGROUND ON REDDIT**

57. Reddit is an online forum owned and operated by the PROVIDER, a company headquartered in San Francisco, California. Reddit users create and moderate online communities known as "subreddits" or "subs." Each subreddit has its own page with a URL in



the format reddit.com/r/sub-reddit-name. Reddit users can post text, video, photos, and links to other websites subject to subreddit rules. Subreddits are moderated by selected users. Reddit users are able to “upvote” and “downvote” content resulting in a cumulative score for content and individual Reddit users known as “karma.” According to the Reddit website, Reddit “is home to thousands of communities, endless conversation, and authentic human connection.”

58. According to Reddit’s law enforcement guide,<sup>9</sup> Reddit collects subscriber information such as subscriber identity, IP logs, email address (if provided), and the user’s name (if provided). Reddit also collects user preference data, account settings, and communication headers, the contents of posts, comments, and “other information regarding the substance of a user’s publicly available communications.” The last category of information is available due to its publicly available nature. Finally, Reddit collects the contents of non-public communications including direct messages, information about a user’s voting, and posts, comments, and other information regarding the substance of a user’s communications on non-public subreddits.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE A SEXUAL  
INTEREST IN CHILDREN OR WHO PRODUCE OR TRAFFIC IN CSAM**

59. Based on my previous investigative experience related to child-exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and/or produce or traffic in CSAM:

- a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children

---

<sup>9</sup> Reddit’s “Guideline for Law Enforcement” is available at [redditinc.com/policies/guidelines-for-law-enforcement](https://www.redditinc.com/policies/guidelines-for-law-enforcement).

engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the

crime is often still discoverable for extended periods of time even after the individual “deleted” it.<sup>10</sup>

f. Such individuals also may correspond with and/or meet others to share information and materials, maintain and conceal such correspondence as they do their sexually explicit material, and often maintain contact information (e.g., online messaging accounts, email addresses, etc.) of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Even if the individual uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in the individual’s home, the SUBJECT ADDRESS, as set forth in Attachment A-I, including on digital devices other than the portable device (for reasons including the frequency of “backing up” or “synching” mobile phones to computers or other digital devices).

60. Based on all of the information contained herein, I believe that Bryan PETERSON, who resides at the SUBJECT ADDRESS and controls the SUBJECT ACCOUNT, likely displays characteristics common to individuals who have a sexual interest in children and/or produce, or

---

<sup>10</sup> See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because “staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology”); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

traffic in CSAM. For example, as noted above, there is probable cause to believe that he is an active participant in Chat Group 1, which is dedicated to discussion of the grooming and sexual exploitation of underage girls and the sharing of pictures depicting such girls, and he made statements indicating that he has had sexual encounters with minors.

### **CONCLUSION**

61. Based on my knowledge, training, experience, and the facts set forth in this affidavit, there is probable cause to believe that the TARGET OFFENSES have been committed and that evidence, fruits, and instrumentalities of those offenses will be found at the SUBJECT ADDRESS, more fully described in Attachment A-I, and within information associated with the SUBJECT ACCOUNT, more fully described in Attachment A-II. Therefore, I respectfully request that this Court issue a search warrant allowing law enforcement to search the locations described in Attachments A-I and A-II and seize the items described in Attachments B-I and B-II.

### **REQUEST FOR SEALING**

62. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is likely unknown to the target of this investigation. Accordingly, there is good cause to seal these documents, as their premature disclosure may alert the targets of this investigation or otherwise seriously jeopardize the investigation.

24-m-617

Davis Mendelsohn

DAVIS MENDELSON

Special Agent

Homeland Security Investigations

Sworn to before me over the telephone and signed by me pursuant to Fed. R. Crim. P. 4.1  
and 4(d) on this 8 day of February 2024.

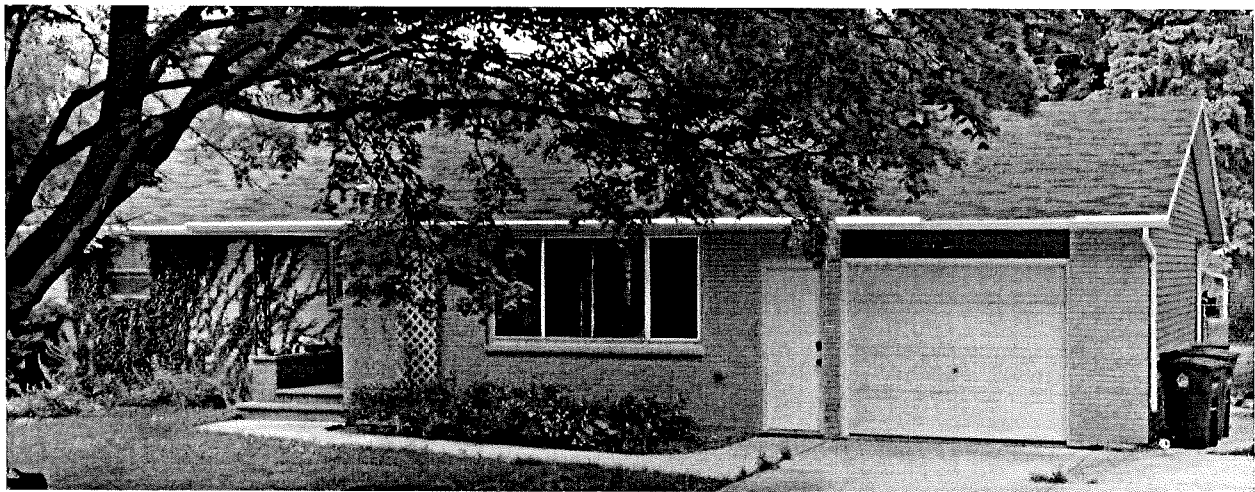
  
HON. JAMES R. SICKEL  
UNITED STATES MAGISTRATE JUDGE



## ATTACHMENT A-I

### **Locations to be searched:**

1. The entire property located at **1210 Valley View Road, Green Bay, WI 54304** (the “**SUBJECT RESIDENCE**”): Pictured below, the SUBJECT RESIDENCE is a single-story residence located on the north side of Valley View Road between Marlee Lane and Orrie Lane in Green Bay, Wisconsin. The SUBJECT RESIDENCE has beige, brick front, red sides, and a gray roof. When looking at the front of the SUBJECT RESIDENCE from Valley View Road, the white, single-car garage is on the right side. There is a red portion above the garage, and the numbers “1210” are affixed to the red portion above the garage. A cement pathway leads from the sidewalk to the four cement steps that precede the SUBJECT RESIDENCE’s front door.



2. The SUBJECT RESIDENCE includes the entirety of the property, including the residence, all rooms, attics, basements, closed and/or locked containers and safes, and other places therein which are part of SUBJECT RESIDENCE and the surrounding grounds, including storage areas, utility sheds, garages, mailboxes, trash containers, appurtenances, outbuildings (whether attached or detached), and vehicles located on the property at the time of the execution of this warrant.

3. A dark gray Ford Escape (Wisconsin license plate AFL3995; vehicle identification number 1FMCU9G91JUB49453) and/or any other vehicles within the Eastern District of Wisconsin at the time this warrant is executed to which law enforcement, through registration documents, car keys, or other specific information, determines Bryan PETERSON has direct access.

4. The property to be searched also includes the person of Bryan PETERSON, whether located at the SUBJECT RESIDENCE or at another location within the Eastern District of Wisconsin at the time this warrant is executed, as well as any computers, cellular telephones, electronic storage media, and other electronic devices found at/in any of the locations searched pursuant to this search warrant.



## **ATTACHMENT B-I**

### **Description of property to be seized:**

1. The following materials which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 371 (conspiracy); 2251(a), (d), and (e) (sexual exploitation of a minor by production and advertisement of child pornography, and conspiracy and attempt to commit such offenses), 2252(a)(1), (a)(2), (a)(4)(B), (b)(1), and (b)(2) (transportation, distribution, receipt, access with intent to view, and possession of child sexual abuse material (“CSAM”), and conspiracy and attempt to commit such offenses); 2252A(a)(1), (a)(2), (a)(3), (a)(5)(B), (b)(1), and (b)(2) (transportation, distribution, receipt, pandering, access with intent to view, and possession of CSAM, and conspiracy and attempt to commit such offenses); and 2422(b) (enticement of a minor to engage in criminal sexual conduct) (collectively, the “TARGET OFFENSES”), including:

- a. Child sexual abuse material and child pornography (as defined in 18 U.S.C. § 2256(8)(a)) and child erotica, in whatever form or medium.
- b. Records and information relating to the production, advertising, transportation, distribution, receipt, transmission, access, editing, creation, possession, or storage of material described in item 1.a, including records and information relating to the identity and location or any person involved in such actions or any person depicted or discussed in such material.
- c. Computers or storage media used to commit the violations described above or that contain any items identified in this Attachment B-1.



d. For any computer or storage medium where seizure is otherwise authorized by this warrant, and any computer or storage medium that contains records or information that is otherwise called for by this warrant (hereinafter, “computer”):

i. Evidence of who used, owned, or controlled the computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chats, instant messaging logs, photographs, and correspondence.

ii. Evidence of software that would allow others to control the computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

iii. Evidence of the lack of such malicious software.

iv. Evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user.

v. Evidence indicating the computer user’s knowledge and/or intent as it relates to the crime(s) under investigation.

vi. Evidence of the attachment to the computer of other storage devices or similar containers for electronic evidence.

vii. Evidence of programs (and associated data) that are designed to eliminate data from the computer.

viii. Evidence of the dates and times the computer was used.

- ix. Passwords, encryption keys, and other access devices that may be necessary to access the computer.
  - x. Documentation and manuals that may be necessary to access the computer or to conduct a forensic examination of the computer.
  - xi. Records of or information about Internet Protocol addresses used by the computer.
  - xii. Records of or information about the computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
  - xiii. Contextual information necessary to understand the evidence described in this attachment.
- e. Routers, modems, and network equipment used to connect computers to the Internet.
- f. Images or information appearing to relate to suspected minors who PETERSON may have solicited or with whom PETERSON may have interacted (including on the computers or storage media as defined herein).
- g. Records, information, and items relating to violations of the statutes described above including:
- i. Records, information, and items relating to the occupancy or ownership of the SUBJECT RESIDENCE including utility and telephone bills, mail envelopes, and addressed correspondence.

ii. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes.

iii. Records and information relating to the identity or location of the persons suspected of violating the statutes described above.

iv. Records and information relating to the sexual exploitation of children.

v. Use of online chat applications, including “Chat Application A,” Reddit, and Snapchat.

2. As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks and other media that can store data), any handmade form (such as writing), any mechanical form (such as printing and typing), and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, and photocopies).

3. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

4. The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macro-SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

5. During the execution of the search of the SUBJECT RESIDENCE further described in Attachment A-I, law enforcement personnel are also specifically authorized to require Bryan PETERSON to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face or iris before the sensor, or any other security feature requiring biometric recognition, of:

- (a) any of the computers found at the SUBJECT RESIDENCE.
- (b) where the computers are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the computers' security features in order to search the contents and applications as authorized by this warrant.

6. This warrant authorizes a review of electronically stored information, communications, and other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

**ATTACHMENT A-II**

This warrant applies to information associated with Reddit account “96jax” (the “SUBJECT ACCOUNT”) that is within the custody or control of Reddit Inc., a company headquartered at 548 Market Street, San Francisco, CA 94104, regardless of where such information is stored, held, or maintained.

## **ATTACHMENT B-II**

### **ITEMS TO BE SEIZED (REDDIT)**

#### **I. INFORMATION TO BE DISCLOSED BY THE PROVIDER**

1. To the extent that the information described in Attachment A-II is within the possession, custody, or control of Reddit, Inc. (the “PROVIDER”), regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each SUBJECT ACCOUNT listed in Attachment A-II:

a. All contents of all wire and electronic communications associated with the SUBJECT ACCOUNT, including:

i. All photographs, images, recordings, emails, communications, or messages of any kind associated with the SUBJECT ACCOUNT, including stored or preserved copies of messages sent to and from the account, deleted or draft messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information associated with each photograph, image, recording, email or message, and any related documents or attachments.

ii. All records pertaining to communications between the PROVIDER and any person regarding the SUBJECT ACCOUNT, including contacts with support services and records of actions taken.

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the

account, the subscriber's full name(s), screen name(s), any alternate names, other account names or email addresses associated with the account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, and including any changes made to any subscriber information or services, including specifically changes made to secondary email accounts, phone numbers, passwords, identity or address information, or types of services used, and including the dates on which such changes occurred, for the SUBJECT ACCOUNT.

ii. All user connection logs and transactional information of all activity relating to the SUBJECT ACCOUNT described above in Section II.1.a., including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dialups, and locations.

iii. Any other account associated with the SUBJECT ACCOUNT including by means of sharing a common device; shared registration IP address; shared email address listed in subscriber records for the account (including any secondary, recovery, fetching, forwarding, or alternate email address); shared phone number or SMS number listed in subscriber records for the account; or accounts connected by cookies or any other means.

iv. Any information showing the location of the user of the SUBJECT ACCOUNT, including while sending or receiving a message using the SUBJECT ACCOUNT or accessing or logged into the SUBJECT ACCOUNT.

## **II. INFORMATION TO BE SEIZED BY THE GOVERNMENT**

2. For each SUBJECT ACCOUNT listed in Attachment A-II, the search team may seize:

a. All information described above in Section I.1.a. that constitutes evidence, contraband, fruits, or instrumentalities of violations of namely violations of Title 18, United States Code, Sections 371 (conspiracy); 2251(a), (d), and (e) (sexual exploitation of a minor by production and advertisement of child pornography, and conspiracy and attempt to commit such offenses), 2252(a)(1), (a)(2), (a)(4)(B), (b)(1), and (b)(2) (transportation, distribution, receipt, access with intent to view, and possession of child sexual abuse material ("CSAM"), and conspiracy and attempt to commit such offenses); 2252A(a)(1), (a)(2), (a)(3), (a)(5)(B), (b)(1), and (b)(2) (transportation, distribution, receipt, pandering, access with intent to view, and possession of CSAM, and conspiracy and attempt to commit such offenses); and 2422(b) (enticement of a minor to engage in criminal sexual conduct) (collectively, the "TARGET OFFENSES"), namely:

i. Child sexual abuse material and child pornography (as defined in 18 U.S.C. § 2256(8)(a)) and child erotica, in whatever form or medium.

ii. Records and information relating to the production, advertising, transportation, distribution, receipt, transmission, access, editing, creation, possession, or storage of material described in item 1.a, including records and



information relating to the identity and location or any person involved in such actions or any person depicted or discussed in such material.

ii. Information relating to who created, accessed, or used the SUBJECT ACCOUNT, including records about their identities and whereabouts.

iii. Information related to how and when the SUBJECT ACCOUNT was accessed or used.

iv. Information, records, messages, communications, audio recordings, pictures, video recordings, or still captured images relating to the account user's or users' communication with suspected minors and/or solicitation of sexually explicit content from minors.

v. Information, in any form, relating to or tending to identify victims of the SUBJECT OFFENSES including records about their whereabouts.

vi. Information, in any form, tending to evidence the age of any suspected victim of the SUBJECT OFFENSES.

b. All records and information described above in Section II.1.b.

#### **IV. PROVIDER PROCEDURES**

3. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the provider shall disclose responsive data by sending it to the following address via US Mail, or to the following email address:

Davis Mendelsohn  
100 Lighthouse Avenue  
Monterey, CA 93940

415-271-6242 (cell)

davis.mendelsohn@ice.dhs.gov

4. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

5. IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 2705(b), that the PROVIDER shall not notify any person, including the subscriber(s) of each account identified in Attachment A-II, of the existence of the warrant, until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date this warrant is signed by the magistrate judge or such later date as may be set by the Court upon application for an extension by the United States. Upon expiration of this order, at least ten business days prior to disclosing the existence of the warrant, the PROVIDER shall notify the agent identified in paragraph 3 above of its intent to so notify.